UCRL-AR-147007

Proper Use of LLNL Computers and Networks-Computer Security Program Policy 2329/4329 v3.0

B. C. Howard, J. D. Day, D. P. Grubb, E. J. Matsche, M. E. Pruitt

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

September 20, 2001

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work was performed under the auspices of the U. S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.

Computer Security Program

Policy
2329 / 4329 v3.0

Proper Use of LLNL Computers and Networks

Statement of Policy

The following rules apply to all users of LLNL classified and unclassified computers and networks; individual organizations may apply additional rules to the use of their resources, provided these additional rules are not in conflict with this policy. Questions concerning organization-specific rules should be addressed to your supervisor, manager, Information System Security Officer (ISSO), or Organizational Information System Security Officer (OISSO).

Please see the References section for additional information pertaining to the following rules.

Authorized Use: Only authorized individuals may use LLNL computers and communication networks.
Unclassified Environment

- LLNL employees who are U.S. citizens are granted access to the institutional unclassified networks and a number of institutional services (e.g., POP accounts for email, LITE for time entry and Meeting Maker for calendaring), as well as to "open access" servers. However, most network services require the user to obtain explicit program authorization before access is allowed.
- Non-employees who are U.S. citizens must receive authorization before using any LLNL unclassified computers or networks. This authorization must come from either the host program or the contract between the Lab and the person's employer.
- Persons who are not U.S. citizens, regardless of employment status, must have approved F-2311 and F-2312 forms in place before using any LLNL unclassified computers or networks. In addition, non-U.S. citizens may only access those computers listed in the approved F-2311 form.

Classified Environment
Prior to being approved for access to a classified resource and annually thereafter, users must:

- complete training on classified computer use in order to achieve and maintain awareness of their responsibilities for protecting classified information systems and classified information; and
- obtain approval for access from the organization responsible for the resource (a record of this approval is retained by the resource’s system administrator and/or ISSO).

Personal Use: Personal use of computers is either limited or prohibited at LLNL, according to the following:
Unclassified Environment
Only LLNL employees may make personal use of LLNL unclassified computing resources, if in accordance with the LLNL Incidental Use Policy P-2023.

Classified Environment

Personal use of LLNL classified computing resources is prohibited.

Authorized Actions: Users of LLNL systems and networks may use those resources only in a manner approved by the institution and their respective programs. Examples of unauthorized actions include, but are not limited to: reading, altering, or destroying information to which the user is not authorized access; and actions that deny legitimate access by authorized personnel to a system or service.

Privacy: Users have limited privacy when using LLNL computers and networks, in accordance with the DOE directive (CIAC Bulletin J-043). This directive is displayed either in hardcopy or as a login banner on all LLNL computers.

Software Licenses: All software used on LLNL computers must be appropriately acquired and used according to the applicable licensing agreements.
Classified Environment
Prior to its installation and use on classified systems, software must be approved (generically or specifically) by the appropriate ISSO. Reference: LLNL Personnel Policies and Procedures Manual Section D VIII.5.

Passwords: Computer passwords must comply with the rules in documents DOE N 205.3 and G 205.3-1.
Classified Environment
Classified computer passwords must also comply with the rules in LLNL Policy P-4310 and DOE M 471.2-2.

Modems: Use of modems is either limited or prohibited at LLNL, according to the following:
Unclassified Environment
The Open Terminal Server (OTS) modem pool is the only approved method of accessing unclassified LLNL computers and networks via modems. All unclassified computer systems with modems, other than Facsimile (FAX) machines, must be configured with auto-answer turned off (see LLNL Policy P-2013).

Classified Environment
Modems are prohibited on classified systems.

Computer Security Incidents: It is the responsibility of all Laboratory employees, contractors, sub-contractors, guests and visitors to report any suspected or actual computer security incident as soon as possible to the ISSO responsible for the resource. The ISSO will report it to LLNL Computer Security Operations (CSO). If the ISSO is not available, then the suspected or actual computer security incident should be reported directly to CSO. CSO will coordinate the investigation with the appropriate internal and external parties (see LLNL Policy P-2316).

Effective Date

This policy is effective on the date of its approval.

Exceptions

Exceptions to this policy may be sought from the CIO by application to the LLNL Computer Security Operations office.

Consequences of Non-Compliance

Failure to comply with this policy, without an approved exception, may result in administrative or corrective actions up to and including dismissal.

Attachments

Glossary

Please see Computer Security Policy Glossary.

Background

The users of LLNL computer systems and networks play a very important role in the overall computer security program at LLNL (see R-1005). To execute this role satisfactorily, users are expected to abide by certain standards of conduct when using those systems. In addition, they must be aware of certain basic expectations and policies governing their use of such systems. This document codifies those standards and expectations.

Implementation and Funding Plan

LLNL will provide an institutional, web-based training course that users of classified resources must complete on an annual basis. LLNL will also maintain records of completion of this course in the central training database.

References

R-1005: Roles and Responsibilities for Unclassified Computer Security

P-2013: Controlling Modem Access to LLNL Computers

P-2023: Incidental Personal Use of Unclassified Information Technology Resources

P-2025: Protecting Unclassified Systems against Viruses and Malicious Code

F-2311: Computer Security Plan for Foreign National Visitors & Employees

F-2312: Computer Security Responsibilities for Hosts of Foreign National Visitors or Assignees

P-2316: Reporting Computer Security Incidents to LLNL Computer Security Operations (CSO)

IM-4310: Classified Computer Password Management Requirements

P-4351: Policy for Protecting Classified Computers from Viruses and Malicious Code at LLNL

Export Control at LLNL

DOE N 205.3 Password Generation, Protection, and Use

DOE G 205.3-1 Password Guide

DOE M 471.2-2 Classified Information Systems Security Manual

Cancellations

P-2329: Computer Use Policy and Security Rules

Policy History

20 Sep 01	Draft v3.0